UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,636	01/16/2004	Monica Ene-Pietrosanu	MS1-1762US	1219

22801 7590 02/10/2009

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
02/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/759,636	ENE-PIETROSANU ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-10 and 13-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-10 and 13-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the amendment filed on 12/1/08.

2. Claims 1-3, 6-10 and 13-43 are pending.

Response to Arguments

3. Applicant's arguments with respect to the prior art rejections of the claims have been considered but are moot in view of the new ground(s) of rejections based on Elgamal and new reference Liu.

Claim Rejections - 35 USC § 101

4. Claims 1-3, 6-10 and 13-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-3, 6-10 and 13-15 define a method comprising establishing at least one cryptographic service parameter; selectively detecting a request for at least one cryptographic service, and selectively performing at least one correctness detection action. However, none of these steps require a specific machine; and there is no transformation of an article or representation of an article (none of "interrupting at least one process"; stopping at least one process"; "starting at least one process"; "suggesting at least one alternative cryptographic service" [see dependent claim 15] are transformations of an article or representations of an article as defined under Bilski) See In re Bilski, 2007-1130 at 15, ("At present, however, and certainly for the present case, we see no need for such a

departure and reaffirm that the machine-or-transformation test, properly applied, is the governing test for determining patent eligibility of a process under § 101." The Court also points to the Abele case where a dependent process claim was determined to be statutory under 101 but not the independent claim; the dependent claim was a sufficiently specific transformation because it changed "raw data into a particular visual depiction of a physical object on a display"; the transformed object must be "physical objects or substances" or "representative of physical objects or substances," id. at 30 and 32).

Claim Rejections - 35 USC § 103

5. Claims 1-3, 6, 7, 10, 13-21, 23-33 and 35-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal et al. US 6,397,330 (hereinafter Elgamal) in view of Liu et al. US 7,051,067 (hereinafter Liu)

6. As per claims 16-21, 23-28 and 42, Elgamal discloses a computer readable medium having computer-implementable instructions embodied thereon, which when executed cause one or more processing units to perform acts comprising:

a. Establishing at least one cryptography service parameter threshold comprising a minimum cryptography service parameter; selectively detecting a request for at least one cryptography service; and selectively performing at least one correctness detection action based on a cryptography service and the at least one cryptography service parameter threshold (Col. 5:60-6:14; 6:19-37 and lines 53-55; 7:11-28 [conformance test parameters defines a min and max

cryptography service parameter]; ("Accordingly, the conformance tests in accordance with the present invention are sufficiently broad to ensure that the cryptographic module is correctly implementing the algorithms and that the key sizes advertised thereform are indeed being used", col. 6:6-10);

b. Establishing at least one maximum cryptography service parameter threshold; (Col. 5:60-6:46)

c. wherein establishing said at least one of either the minimum or maximum cryptography service parameter threshold includes at least one of the following acts: identifying unacceptable cryptography algorithms; and identifying acceptable cryptography algorithms (6:26-27 and lines 57-60; 7:15-17 and lines 22-28);

d. wherein establishing said at least one of either the minimum or maximum cryptography service parameter threshold includes at least one of the following acts: identifying at least one unacceptable cryptography key size parameter; and identifying at least one acceptable cryptography key size parameter (5:66-6:2; 6:25-31 and lines 53-56);

e. wherein establishing said at least one of either the minimum or maximum cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier (6:57-65; 8:1-34 "Table 2");

f. wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories comprising authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms (5:66-6:2; 6:25-37);

g. wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface. (5:60-61; 6:19-21)

h. wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold (6:2; 6:25-31);

i. wherein determining if said cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold includes comparing a size of said cryptographic key with said at least one cryptography service parameter threshold (6:2; 6:25);

j. wherein selectively performing said at least one correctness detection action if said cryptography service does not satisfy said at least one cryptography

service parameter threshold includes determining if a cryptographic algorithm associated with said cryptography service is suitable for use based on said at least one cryptography service parameter threshold (5:66-6:4; 6:25-35; 7:15-20);

k. wherein determining if said cryptographic algorithm associated with said cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold (5:66-6:4; 6:25-35; 7:15-20);

l. wherein selectively performing said at least one correctness detection action based on said cryptography service if said cryptography service does not satisfy said at least one cryptography service parameter threshold includes performing at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, and causing alteration of a graphical user interface (6:3-4, 30 and lines 57-60);

m. wherein: the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and the selectively performing at least one correctness detection action based on the cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the cryptography service is suitable for use based on the at least one cryptography

service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length. (6:6-10; conformance tests ensure that the cryptographic module is correctly implementing the algorithms and that the advertised key sizes).

7. Elgamal does not disclose wherein the step of selectively performing at least one correctness detection action is based on the requested cryptography service and the at least one cryptography service parameter threshold; wherein the at least one correctness detection action selectively performing includes forcing use of at least one alternative cryptographic service. Liu discloses an object oriented mechanism for dynamically constructing customized cryptographic service implementations on a per request basis, wherein the mechanism checks for a general implementation of a service, and if a general implementation of a service is found, the mechanism then determines if the implementation is authentic. (6:5-31) If the general implementation of the service is not found to be authentic, the mechanism checks for another general implementation, and so on until either one is found that is authentic or none are found that are authentic. (6:32-59) If an authentic general implementation is found, then the mechanism determines whether there are any restrictions that need to be imposed on the implementation, and whether there are any exemptions. (6:59-7:26) Liu further discloses the step of determining whether a general implementation of a service is

authentic in broad terms: including soliciting expected information from the general implementation to ensure that the implementation is legitimate. (Col. 18:45-19:32) It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the step of selectively performing at least one correctness detection action to be based on the requested cryptography service and the at least one cryptography service parameter threshold; and wherein the at least one correctness detection action selectively performing includes forcing use of at least one alternative cryptographic service. One would be motivated to do so to provide a conformance test on a per request basis, and to provide an alternative service when a prior selected service does not pass a conformance test as suggested by Liu, ibid. The aforementioned cover the limitations of claims 16-21, 23-28 and 42.

8. As per claims 1-3, 6, 7, 10 and 13-15, they are method claims corresponding to claims 16-21, 23-28 and 42. In addition, Elgamal in view of Liu suggest wherein the alternative cryptography service comprises a cryptography service which meets the minimum level of security. (an alternative service defined by the policy file will meet all the conformance parameters) It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the at least one correctness detection action selectively performed includes suggesting at least one alternative cryptographic service. One would be motivated to do so to ensure that the client receives a viable alternative service if the initial requested service does not conform as known to one of ordinary skill in the art and as suggested by Liu, ibid. Therefore, claims 1-3, 6, 7, 10 and 13-15 are

rejected as being unpatentable over Elgamal in view of Liu for the same reasons set forth in the rejections of claims 16-21, 23-28 and 42.

9. As per claim 41, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Elgamal in view of Liu is incorporated herein. Although neither Elgamal nor Liu expressly teach in an event that the cryptography service is an asymmetric cryptography service, the minimum level of security comprises a minimum acceptable public key size of at least 1024 bits; and in an event that the cryptography service is a symmetric cryptography service, the minimum level of security comprises a minimum acceptable symmetric key size of at least 128 bits; it was notoriously well known at the time the invention was made that secure asymmetric keys where at least 1024 bits in length and secure symmetric key required at least 128 bits. For example, RSA encryption techniques typically utilized 1024 bit keys and DES typically implemented 128 bit keys. Official Notice of this fact is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein in an event that the cryptography service is an asymmetric cryptography service, the minimum level of security comprises a minimum acceptable public key size of at least 1024 bits; and in an event that the cryptography service is a symmetric cryptography service, the minimum level of security comprises a minimum acceptable symmetric key size of at least 128 bits because these were known in the art to be the minimum key lengths to ensure secure cryptographic services. The aforementioned cover the limitations of claim 41.

10. As per claims 29-33, 35-40 and 43, they are apparatus claims corresponding to claims 16-21, 23-28 and 42. In addition, Elgamal discloses cryptography correctness detection logic configured to perform the acts listed in claims 16-21, 23-28 and 42, and moreover, Elgamal discloses memory operatively coupled to the correctness detection logic, wherein the cryptography service parameter threshold is in the memory. (fig. 1, "Policy Filters" and related text) Furthermore, Elgamal in view of Liu suggest selectively perform at least one correctness detection action based on the requested cryptography service if the requested cryptography service does not satisfy the at least one cryptography service parameter threshold, wherein the at least one correctness detection action selectively performed includes forcing use of at least one other cryptography service, wherein the at least one other cryptography service comprises a cryptography service having a higher level of security than represented by the cryptography service parameter threshold. (A request for a cryptographic service that did not pass the conformance test is replaced by an alternative cryptographic service that did pass its conformance test) It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the at least one correctness detection action selectively performed includes forcing use of at least one alternative cryptographic service. One would be motivated to do so to ensure that the client receives a viable alternative service if the initial requested service does not conform as known to one of ordinary skill in the art and as suggested by Liu, ibid. As such, claims 29-33, 35-40 and 43 are rejected as being unpatentable over Elgamal in view of Liu.

11. Claims 8, 9, 22 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Liu, and further in view of Fielder et al. US 5,963,646 (hereinafter Fielder).

12. As per claim 22, the rejection of claim 17 under 35 USC 103(a) as being unpatentable over Elgamal in view of Liu is incorporated herein. In addition, Elgamal discloses disabling a crypto module if the module does not correctly implement the algorithms and/or key sizes configured, and removing unauthorized cipher suites, wherein a cipher suite is a collection of encryption algorithms, key sizes, and parameters that specifies the type and strength of a particular cryptographic operation. (Col. 5:66-6:5; 6:25-31) Elgamal does not expressly disclose, wherein establishing said at least one of either the minimum or maximum cryptography service parameter threshold includes at least one of the following acts: identifying at least one acceptable seed size parameter; and identifying at least one unacceptable seed size parameter. However, it is well known in the art at the time of invention that the length or size of a seed value, which is used to generate a cryptographic key directly, corresponds to the cryptographic strength of the key value used in a cipher function. For example, Fielder discloses a key generator that takes as inputs one or more seed values to generate a deterministic encryption key. Fig. 2. Fielder further discloses that the size of the seed value has a direct relationship to the strength of the generated encryption key. Col. 5:54-6:4. Hence, a seed value is a significant parameter that specifies the type and

strength of a particular cryptographic operation. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the act of establishing the at least one cryptographic service parameter threshold as disclosed by Elgamal to include at least one of the following acts: identifying at least one acceptable seed size parameter; and identifying at least one unacceptable seed size parameter. One would be motivated to do so because seed size directly corresponds to the strength of a particular cryptographic operation as taught by Fielder and as known to one of ordinary skill in the art. The aforementioned covers the limitation of claim 22.

13. As per claims 8 and 9, they are method claims corresponding to claim 22, and they do not teach or define above the information claimed in claim 22. Therefore, claims 8 and 9 are rejected as being unpatentable over Elgamal in view of Liu and Fielder for the same reasons set forth in the rejection of claim 22.

14. As per claim 34, it is an apparatus claims corresponding to claims 22 and 30, and it does not teach or define above the information claimed in claims 22 and 30. Therefore, claim 34 is rejected as being unpatentable over Elgamal in view of Liu and Fielder for the same reasons set forth in the rejection of claim 22 and 30.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432